IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application Of:	§	**Atty. Docket No. RPS920030206US2**
	§	
RYAN CHARLES CATHERMAN	§	**Examiner: TURCHEN, JAMES R.**
	§	
Serial No.: 10/749,261	§	**Art Unit: 2139**
	§	
Filed: DECEMBER 31, 2003	§	**Conf. no.: 8466**
	§	
For: METHOD FOR SECURELY CREATING AN ENDORSEMENT CERTIFICATE UTILIZING SIGNING KEY PAIRS	§	

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF UNDER 37 C.F.R. §41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Supplemental Appeal Brief is submitted in response to a Notification of Non-Compliant Appeal Brief ("Notification") dated October 26, 2009 with respect to the Appeal Brief filed on November 26, 2009. The present Supplemental Appeal Brief corrects the deficiencies noted by Examiner within the previous submission. No fees are believed to be due at this time, however, please charge any fees necessary to further the prosecution of this application to **Deposit Account Number 50-3083**.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As recited by Appellants' example method Claim 1, Appellants' invention provides a method (FIGs. 4 and 5) for securely creating an endorsement certificate for a device in an insecure environment. The method comprises: generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices (*see* ¶ 0040, 0041). The method further comprises: verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶ 0045, 0046; FIG. 4, 415, 416); and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the method further comprises immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

Appellants' Claim 12 and 13 further provides a data processing system comprising: a processor 150; a trusted platform module (TPM) chip 150; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server 107; and means, whereby said TPM 150 is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture (103) of the TPM, wherein said signing key pair is a single-use parameter (¶ 0044),

said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK (¶ 0044). The signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM (¶ 0045). The means for verifying an endorsement key pair further comprises: means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed (EK) (¶¶ 0045-0046); and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate (¶¶ 0045-0047; FIG. 4; *see* also FIG. 5, ¶¶ 0049-0051).

Similarly, Claim 14 provides a data processing system 104 utilized for issuing endorsement certificates. The data processing system 104 comprises: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key. Further, the data processing system comprises program means for: determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices; recording when a request for EK certificate fails (FIG. 4, 423; ¶ 48; *see* also FIG. 5, ¶¶ 0049-0051); tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and messaging said TPM vendors to update their security procedures (*id.*).

As recited by Appellants' example system Claim 17, Appellants' invention provides a system (FIGs. 1, 2 and 3) for securely creating an endorsement certificate for a device in an insecure environment. The system comprises: means for generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); means for creating a non-public, signing key

pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number of devices from the plurality of valid devices (*see* ¶¶ 0040, 0041). The system further comprises: means for verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶¶ 0045, 0046; FIG. 4, 415, 416); and means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the system further comprises means for immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

CONCLUSION

Appellants further respectfully request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

/Eustace P. Isidore/

Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS